REMARKS

The Office Action dated December 11, 2009 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 7, 8, 10, 14, 20, 24, 28, 30, 31, 35 and 36 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 21 and 22 have been canceled without prejudice or disclaimer. No new issues have been raised. Claims 1-10, 14-20 and 23-39 are presently pending.

The Office Action indicated that claims 21, 22, 27, 28, 34 and 35 have been allowed. Applicants wish to thank the Examiner for allowing these claims. Applicants have cancelled claims 21 and 22 and have incorporated certain subject matter from claims 21 and 22 into independent claims 14, 24 and 31. In addition, Applicants submit that all currently pending claims are in condition for allowance. Claims 1-20, 23-26, 29-33 and 36-44 are respectfully submitted for reconsideration.

The Office Action rejected claims 1 and 14 under 35 U.S.C. §101 for allegedly being directed to non-statutory subject matter. Specifically, it was alleged that claims 1 and 14 are not tied to a statutory class of invention. Applicants have amended claims 1 and 14 to recite a "network element" that is tied to the extracting of the routing information, and, additionally, the subsequent generating, replacing and forwarding operations. The network element is the statutory class of invention that is at the border between the two networks, and, thus is tied to each of the recited method operations.

Accordingly, Applicants submit that claims 1 and 14 are in compliance with 35 U.S.C. §101. Withdrawal of the rejection is kindly requested.

Claims 1-2, 7-10, 13, 14, 20, 23, 24, 29-31 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Irwin (U.S. Patent Publication No. 2003/0204728) in view of Siegel (U.S. Patent Publication No. 2004/0203799). The Office Action took the position that Irwin discloses all of the elements of the claims except for routing information in the received packet. The Office Action then relied on Siegel as allegedly curing the deficiencies of Irwin with respect to the pending claims. This rejection is respectfully traversed for at least the following reasons.

Claim 1, from which claims 2-9 depend, is directed to a method. Routing information is extracted at a network element from a received message at a border between a first network and a second network. At least one invalid routing entry is added to first-network routing entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network routing entries relate to a routing path of the message within the first network. An encrypted routing information is generated by encrypting the at least one invalid routing entry and the first-network routing entries by using an own token at least for each of the first-network routing entries. Routing information of the received message is replaced by the encrypted routing information. The received message is forwarded with the encrypted routing information to the second network.

Claim 10 is directed to an apparatus. An extracting means is configured for extracting the routing information from a received message at a border between a first network and a second network. An adding means is configured for adding at least one invalid routing entry to first-network routing entries of the routing information in order to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network routing entries relate to a routing path of the message within the first network. An encrypting means is configured for generating an encrypted routing information by encrypting the at least one invalid routing entry and the first-network routing entries by using an own token at least for each of the first-network routing entries. A replacing means is configured for replacing the routing information of the received message by the encrypted routing information. A forwarding means is configured for forwarding the received message with the encrypted routing information to the second network.

Claim 14, from which claims 15-23 depend, is directed to a method. Routing information is extracted at a network element from a received message at a border between a first network and a second network. A decrypted and reversed routing information is generated by decrypting a tokenized second-network routing entry relating to a routing path of the message within the second network. The content of the decrypted second-network routing entry is also reversed. The routing information of the received message is replaced by the decrypted and reversed routing information. The received message is forwarded with the decrypted and reversed routing information to the second

network. The method also includes marking a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node, and performing at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network routing entries at incoming tokenizing network nodes before encryption

Claim 24, from which claims 25-29 depend, is directed to an apparatus. An extracting means is configured for extracting routing information from a received message at a border between a first network and a second network. A decrypting and reversing means is configured for generating decrypted and reversed routing information, by decrypting a tokenized second-network routing entry relating to a routing path of the message within the second network, and reversing the content of the decrypted second-network routing entry. A replacing means is configured for replacing the routing information of the received message by the decrypted and reversed routing information. A forwarding means is configured for forwarding the received message with the decrypted and reversed routing information to the second network. The apparatus also includes marking means for marking a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node, and at least one of suppressing means for suppressing said reversing at outgoing tokenizing network nodes and reversing means for reversing network routing entries at incoming tokenizing network nodes before encryption.

Claim 30, from which claims 37-39 depend, is directed to an apparatus. An extractor is configured to extract routing information from a received message at a border

between a first network and a second network. An adder, operably connected to the extractor, is configured to add at least one invalid routing entry to first-network routing entries of the routing information to blurr or hide an actual number of routing entries which correspond to routing nodes through which the received message has been routed. The first-network routing entries relate to a routing path of the message within the first network. An encryptor, operably connected to the extractor, is configured to generate encrypted routing information by encrypting the at least one invalid routing entry and the first-network routing entries, by using an own token at least for each of the first-network routing entries. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the encrypted routing information. A transmitter, operably connected to the extractor, is configured to forward the received message with the encrypted routing information to the second network.

Claim 31, from which claims 32-36 depend, is directed to an apparatus. An extractor is configured to extract the routing information from a received message at a border between a first network and a second network. A decryptor, operably connected to the extractor, is configured to generate a decrypted and reversed routing information by decrypting a tokenized second-network routing entry relating to a routing path of the message within the second network and further configured to reverse the content of the decrypted second-network routing entry. A replacer, operably connected to the extractor, is configured to replace the routing information of the received message by the decrypted and reversed routing information. A transmitter, operably connected to said extractor, is

configured to forward the received message with the decrypted and reversed routing information to the second network. The apparatus also includes a marker configured to mark a tokenized network routing entry of at least one of an incoming and an outgoing tokenizing network node, and a processor configured to perform at least one of suppressing said reversing at outgoing tokenizing network nodes and reversing network routing entries at incoming tokenizing network nodes before encryption.

As will be discussed below, the teachings of Irwin and Siegel, taken individually or in combination, fail to disclose or suggest all of the elements of the claims, and therefore fails to provide the features discussed above. The rejection is respectfully traversed for at least the following reasons.

Initially, Applicants note that independent claims 14, 24 and 31 have been amended to recite certain features from allowable claims 21 and 22, which are now cancelled. Accordingly, Applicants submit that the rejections of independent claims 14, 24 and 31 and those claims dependent thereon are moot. An allowance of each of claims 14, 24 and 31 and those claims dependent thereon is respectfully requested.

As for the rejection of claims 1-10 and 30, Applicants offer the following comments.

Irwin discloses a method of cryptography that generates a special value that relates to a communications packet. The special value is hidden in a field of a packet header of a communications packet. Referring to FIG. 1, a source node 12 is connected to an intermediary node 14 via a communications link 16. The source node 12 computes a

cryptographic special value 30 for each packet to be transmitted by using a shared secret key (SSK) that is know by the source node 12 and intermediary node 14. The special value 30 is hidden in one or more fields 26 within the header portion 22 of each packet to be transmitted (see paragraph [0022] of Irwin). The packet 20 is then transmitted over the network 18 towards the destination node 14. The destination node 14 will compute a cryptographic special value 30' using the shared secret key and will compare the special value 30' to the original special value received 30. If the special values (30 and 30') match, the destination intermediary node 14 has successfully authenticated the transmitted packet 20.

Irwin discloses that authentication of a communications packet originates from a certain source node that hides a cryptographically generated first special value in a header portion of the packet (see Abstract of Irwin). Claim 1 recites "adding at least one invalid routing entry to first-network routing entries of said routing information to blur or hide an actual number of routing entries...said first-network routing entries relating to a routing path of said message within said first network...generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries...replacing said routing information of said received message by said encrypted routing information." Applicants submit that Irwin fails to disclose the above-noted features of independent claim 1 and similarly independent claims 10 and 30.

According to the FIG. 2 and paragraph [0052] of the present application (or paragraphs [0127] to [0139] of the published application US 2005/0083974 A1), a record-route is illustrated that includes additional invalid routing entries, such as, "token(invalid)@home2.net;tokenizedby=home2.net." This example entry is clearly designated as an "invalid" entry and thus represents an invalid routing entry.

Applicants have amended the claims to recite that the invalid entry is the "invalid routing entry", similar to what is disclosed in paragraph [0051] of the present application. Irwin does not disclose any invalid routing entry. The "special value" disclosed in Irwin is not comparable to the invalid routing entries of the present application.

Referring to paragraphs [0020] through [0022] of Irwin

> "The header portion 22 contains a number of fields 26. Examples of such fields for an IP packet may include an origination field (identifying the source node 12), a destination field (identifying the destination node 14), an identification (ID) field, and the like...This header portion 22, like that with the IP packet, also contains fields 26, and these included fields may provide, for example, destination and origination port information...With reference once again to FIG. 1, the steganography process of the present invention generally operates at the source node 12 to compute 28 a cryptographic special value 30 for each packet to be transmitted...the special value 30 placed in the field(s) 26 should possess the characteristics of the commonly used field value. By this it is meant that the special value 30 should have the same number of bits, same general format, same general range, and the like, as the value that is commonly found in that field (or fields) 26 of the header portion 22."

As may be clearly observed from the above-noted portion of Irwin's disclosure, the special value 30 does not include any invalid routing entry or even arguably comparable

entry. At best, the special value 30 is a modified version of the header portion 22, which includes typical and conventional header information.

Contrary to the subject matter recited in Irwin, claim 1 recites "adding at least one "invalid routing entry to first-network routing entries." This effectively increases the number of routing entries, and, blurs or hides an actual number of routing entries that correspond to routing nodes through which the received message has been routed. As a result, the number of routing entries corresponds to the sum of the at least one invalid routing entry, and, the actual number of routing entries corresponds to the routing nodes.

Irwin does not disclose or suggest "adding at least one invalid routing entry to first-network routing entries of said routing information to blur or hide an actual number of routing entries...said first-network routing entries relating to a routing path of said message within said first network...generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries...replacing said routing information of said received message by said encrypted routing information", as recited in independent claim 1 and similarly in independent claims 10 and 30. Applicants submit that Siegel fails to cure the deficiencies of Irwin with respect to any of independent claims 1, 10 and 30.

Siegel merely discloses that header routing information is extracted from a voice message. Also, routing information may be modified and then replaced in the voice message. However, the modification is performed for routing optimization purposes. The

Office Action relied on Siegel to disclose simply forwarding the received message with the encrypted routing information.

There is no disclosure in Siegel of any invalid routing entry. Like Irwin, Siegel does not disclose or suggest "adding at least one invalid routing entry to first-network routing entries of said routing information to blur or hide an actual number of routing entries...said first-network routing entries relating to a routing path of said message within said first network...generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries...replacing said routing information of said received message by said encrypted routing information", as recited in independent claim 1 and similarly in independent claims 10 and 30. Applicants submit that Siegel is limited to mere extraction of routing information from a voice message. Siegel does not disclose any adding of an invalid routing entry, and, especially, not adding invalid routing entry information to blur or hide an actual number of routing entries.

Therefore, Applicants submit that Irwin and Siegel, taken individually or in combination, fails to disclose all of the subject matter of independent claims 1, 10, 14, 24, 30 and 31. By virtue of dependency, Irwin also fails to teach the subject matter of dependent claims 2-9, 15-20, 23, 25-29, and 32-39. Withdrawal of the rejection of claims 1, 2, 7-10, 13, 14, 23, 24, 29-31 and 36 is kindly requested.

Claims 3, 11, 16 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Irwin in view of Siegel and further in view of Yla-Outinen et al. (U.S. Patent Publication No. 2004/0152469). This rejection is respectfully traversed. Claim 11 has been cancelled thus rendering its rejection moot.

Irwin and Siegel are discussed above. Yla-Outinen discloses a method and a system for controlling a processing load in a packet data network, wherein a load control information is set in a predetermined field of a message. The load control information is then checked on the routing path of the message and a processing resource of the packet data network is selected in response to the result of a checking step. Load balancing information can be provided at the network to provide a balancing and load sharing function without heavy string comparisons and data base queries.

Claims 3, 16 and 25 are dependent upon claims 1, 14 and 24 and contain all of the limitations thereof. As discussed above, Irwin and Siegel fail to disclose or suggest all of the elements of claims 1, 14 and 24. In addition, Yla-Outinen fails to cure the deficiencies in Irwin as Jensen also fails to disclose or suggest "adding at least one invalid routing entry to first-network routing entries of said routing information to blur or hide an actual number of routing entries...said first-network routing entries relating to a routing path of said message within said first network...generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries...replacing said routing information of said received message by said encrypted

routing information", as recited in independent claim 1 and similarly in independent claims 10 and 30. Thus, the combination of Irwin and Yla-Outinen fails to disclose or suggest all of the elements of claims. Furthermore, claims 3, 16 and 25 should be allowed for at least their dependence upon claims 1, 14 and 24 and for the specific limitations recited therein.

Claims 4-6 and 17-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Irwin in view of Siegel and further in view of Jensen et al. (U.S. Patent No. 6,185,612). This rejection is respectfully traversed.

Irwin and Siegel are discussed above. Jensen discloses a method for managing and using topology information in a network. A topology information manager keeps fragments of network topology and provides access to entire fragments or to fragment summaries in response to authenticated requests. An authenticated path selector uses topology information from the manager to select message routes. The path selector may use summaries of hidden network paths to determine whether the hidden path is desirable, without having access to all topological information about the hidden path. Messages may be forwarded over hidden paths by the manager without disclosing more than the summary information to the message provider.

Claims 4-6 and 17-19 are dependent upon claims 1 and 14 and contain all of the limitations thereof. As discussed above, Irwin and Siegel fail to disclose or suggest all of the elements of claims 1 and 14. In addition, Jensen fails to cure the deficiencies in Irwin as Jensen also fails to disclose or suggest "adding at least one invalid routing entry to

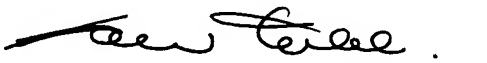
first-network routing entries of said routing information to blur or hide an actual number of routing entries...said first-network routing entries relating to a routing path of said message within said first network...generating an encrypted routing information by encrypting said at least one invalid routing entry and said first-network routing entries by using an own token at least for each of said first-network routing entries...replacing said routing information of said received message by said encrypted routing information", as recited in independent claim 1 and similarly in independent claims 10 and 30. Thus, the combination of Irwin, Siegel and Jensen fails to disclose or suggest all of the elements of claims. Furthermore, claims 4-6 and 17-19 should be allowed for at least their dependence upon claims 1 and 14 and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited references fail to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-10 and 14-20 and 23-36 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Kamran Emdadi
Registration No. 58,823

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

KE:sjm

Enclosures: Petition for Extension of Time
Check No. 20850